Physical and Environmental Security Procedure

Version 1 - Approved by Youssef Ouyhya

Contents

1. Objective

An Information Security Management System (ISMS) has been implemented at CNTXT to protect the organization's sensitive information from unauthorized access, loss, or inaccuracy.

Through this document, CNTXT has recognized the need and established guidelines to incorporate physical and environmental security to prevent unauthorized access to physical spaces, avoid damage to assets and prevent interference with the company’s information and information processing facilities.

2. Scope

The scope of the Physical and Environmental Security procedure is limited to the production environment facilities, their supporting functions, and physical assets.

3. Process Responsibilities

3.1 Information Security Officer

Reviewing the device security status checks.

3.2 Engineering Department and HR

- Allocation and deallocation of systems/devices.
- Training of users regarding the use of physical assets like Laptops.
- Ensuring that the return of information assets and removal of access to systems is done appropriately.

4. Physical Security Requirements

- CNTXT is a “software as a service” (SaaS) company; a third-party infrastructure provider is hosting the production infrastructure of CNTXT.
- It is the responsibility of the Information Security Officer, with help from the legal and engineering team, to review the agreements annually and collects vendor’s certificates or security reports (ISO certificate and SOC 2 report) to ensure the credibility of the Infrastructure provider to protect the confidentiality, integrity, and availability of CNTXT’s data.
- The physical office premises are outside the scope of the ISMS since no production servers or customer data are hosted at our office premises.

5. Requirement for Physical Assets

- It is the responsibility of each user to protect assets with due importance given to their security.

- It is the responsibility of HR to ensure staff with access to assets i.e., laptops shall be made aware of the information security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection through periodic ISMS training and awareness programs and as per the asset management policy and HR security policy.
- All employees shall be made aware not to leave equipment unattended. Personnel shall be aware to terminate active sessions when finished unless they can be secured by an appropriate locking mechanism. Examples include using password-protected screen savers, log-off from applications when no longer needed, securing laptops or mobile devices from unauthorized use by a password, etc. Personnel shall be made aware of these practices through Information Security Policies and Procedures.

6. Clear Desk & Clear Screen Policy

Clear Desk Policy applies to paper (hardcopy) and laptops to ensure unauthorized personnel do not have access to CNTXT information. While it is strongly recommended not to use paper assets – in cases where it is required, the following will be applicable:

6.1 Clear Desk Policy

- Client Confidential / CNTXT Confidential paper assets (project-specific or product development papers) shall not be left unattended to avoid access by unauthorized personnel.
- Passwords must always be memorized and must never be written down on paper.
- All workspaces must always be left clear before leaving for longer periods of time.
- In case of an incident associated with information loss, the matter must be immediately escalated to the Information Security Officer and should follow the Incident Management Procedure.

6.2 Clear Screen Policy

- Users shall lock their computers when leaving their desks and log off when leaving for an extended period of time. This ensures that the contents of the computer screen are protected from prying eyes, and the computer is protected from unauthorized access.
- Use of Laptop / Desktop Privacy Screens shall be considered in case required.
- Users shall not keep files/shortcuts on the desktop screen; and
- Users shall delete all the files from the recycle bin on a regular basis.

7. Document Security Classification

Company Internal (please refer to the Data Classification policy for details).

8. Non-Compliance

Compliance with this policy shall be verified through various methods, including but not limited to automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

9. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

10. Schedule

This document is to be reviewed annually and whenever significant changes occur in the organization.

End of Physical & Environmental Security Procedure. For version history, please see the next page.

Version history

Version	Log	Date
1 Current	Policy version approved by Youssef Ouyhya	26 Oct, 2024
1	New Policy version Created	26 Oct, 2024